REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

Independent claims 40, 53, and 65 have been amended to introduce the recited initials "PSD" with the full nomenclature personal security device (PSD) and thereby clarify the claims. The amendments do not narrow the scope of the claims; therefore, no estoppel is deemed attachable thereto.

Claims 40-58, 60-62, and 64-71 stand rejected, under 35 USC §102(e), as being anticipated by Sigaud (US 6,657,956). Claim 63 stands rejected, under 35 USC §103(a), as being unpatentable over Sigaud. Claim 59 stands rejected, under 35 USC §103(a), as being unpatentable over Sigaud in view of Boyles et al. (US 6,738,901).

The Applicants respectfully traverse the rejections.

Sigaud discloses a data processing system that performs authentication and business transactions (see Sigaud title and abstract). The data processing system includes a local client 2 that supports a network connection 42. An authentication server 1 performs authentications according to a predetermined authentication policy 15 and supports a network connection 40, 42. An intelligent device 21 supports a PSD 22 and a device connection 20. PSD 22 is functionally connected to intelligent device 21 and configured to generate authentication information

according to predetermined authentication policy 15, which is shared by the local client within application security software 27. As illustrated in Sigaud's Fig. 1, local client 2 and authentication server 1 are functionally connected to each other over a network connection 42.

The invention defined by claim 40 differs from Sigaud's system in that for the claimed subject matter:

- the intelligent device is portable;

- the intelligent device is configured to further support a network connection;

- the predetermined authentication policy is functionally stored within the PSD and the authentication server; and

- the local client comprises an activator of an authentication according to the authentication policy between the PSD and the authentication server upon an action of an identified user on the local client.

By contrast to the above-noted claimed subject matter, Sigaud discloses that reader 21 is linked to local client 2 via physical link 20. Therefore, reader 21 is not portable. Moreover, reader 21 is not configured to have a network connection. Furthermore, Sigaud discloses that the predetermined authentication policy is functionally stored within the local client and the authentication server. Still further, Sigaud

discloses that the activator of an authentication policy is not implemented in the local client but in the authentication server (Sigaud col. 4, lines 4-59).

Claim 40 further distinguishes over Sigaud's disclosure in that the claimed authentication is performed between the PSD and the authentication server upon an action of an identified user on a local client. The identified user is associated with the PSD, and the PSD uses a portable intelligent device as a communication interface. Therefore, the identified user, while trying to do an action on a local client, is authenticated by the intelligent portable device, since the PSD is functionally connected to the intelligent portable device and not necessarily to the local client. This feature solves the problem cited in page 1, lines 23-28, of the current application and constitutes a major difference between Sigaud and the claimed invention.

In accordance with the above discussion, the Applicants submit that Sigaud does not anticipate the subject matter defined by claim 40. Claim 53 similarly recites the features distinguishing apparatus claim 40 from Sigaud, although with respect to a method. Claims 53 is therefore allowable for similar reasons that claim 40 is allowable.

Therefore, allowance of claims 40 and 53 and all claims dependent therefrom is warranted.

Dependent claim 45 recites that the intelligent portable device of base claim 40 is connected to the authentication server through a network connection and configured as an independent portable device. The claimed features allow the PSD to communicate the authentication information to the authentication server independently of a local client. These feature and the advantage they provide are not possible in Sigaud's structure because Sigaud's reader 21 is physically linked 20 to local client 2. Accordingly, allowance of claim 45 is warranted for this independent reason.

Dependent claim 47 recites that the intelligent portable device of base claim 40 and intervening claim 45 may be connected to the authentication server through two network connections using two networks. This feature cannot be achieved by Sigaud's structure because Sigaud's reader 21 is physically linked 20 to local client 2. Accordingly, allowance of claim 47 is warranted for this independent reason.

Dependent claim 54 recites that an authentication request, sent by the local client defined in base claim 53, has a unique identifier associated with the identified user. This identifier enables the authentication server to communicate with the proper PSD. The Final Rejection does not propose that Sigaud expressly

discloses this feature. Accordingly, allowance of claim 54 is warranted for this independent reason.

Dependent claim 55 recites that a unique identifier is used by the authentication server, of base claim 53 and intervening claim 54, for locating and communicating with the intelligent portable device associated with the identified user. Therefore, a communication between the authentication server and the local client for the authentication process is not mandatory. By contrast to this feature, Sigaud discloses that the authentication server needs local client 2 to communicate with PSD 22 via reader 21 and physical link 20. Accordingly, allowance of claim 55 is warranted for this independent reason.

Independent claim 65 recites an intelligent portable data processing device that differs from Sigaud's reader 21, in that the claimed intelligent portable device:

- is portable;

- is configured to support a network connection;

- shares a predetermined authentication policy with a remote authentication server; and

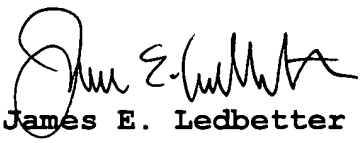
- is configured to transfer, to an associated PSD, a received request for authentication, upon receiving the request, if the request contains an identifier associated with the PSD.

For analogous reasons to those provided in connection with the claims discussed above, which recite features similar to those identified immediately above for distinguishing claim 65, Sigaud does not anticipate the subject matter defined by claim 65. Therefore, allowance of claim 65 and all claims dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



Date: October 27, 2005
JEL/DWW/att

James E. Ledbetter
Registration No. 28,732

Attorney Docket No. L741.01104
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200